Feuille de TD n°5

MP Clemenceau

Octobre 2022

1 Banque CCP

Exercice 1 :

1) Soit $(a,b,p) \in \mathbb{Z}^3$. Prouver que si $p \wedge a = 1$ et $p \wedge b = 1$, alors $p \wedge (ab) = 1$.

2) Soit p un nombre premier.

(a) Prouver que $\forall k \in [\![1, p-1]\!]$, p divise $\binom{p}{k} k!$ puis que p divise $\binom{p}{k}$.

(b) Prouver que : $\forall n \in \mathbb{N},\ n^p \equiv n \mod p$.
Indication : Procéder par récurrence.

(c) En déduire que : $\forall n \in \mathbb{N}$, p ne divise pas $n \Longrightarrow n^{p-1} \equiv 1 \mod p$.

Exercice 2 :

1) Énoncer le théorème de Bézout dans $\mathbb{Z}$.

2) Soit a et b deux entiers naturels premiers entre eux.
Soit $c \in \mathbb{N}$.
Prouver que : $(a|c \text{ et } b|c) \Longleftrightarrow ab|c$.

3) On considère le système $(S) : \begin{cases} x \equiv 6 \mod(17) \\ x \equiv 4 \mod(15) \end{cases}$ dans lequel l'inconnue x appartient à $\mathbb{Z}$.

(a) Déterminer une solution particulière x_0 de (S) dans $\mathbb{Z}$.

(b) *Déduire des questions précédentes* la résolution dans $\mathbb{Z}$ du système (S).

2 Groupes

Exercice 3 : Un sous groupe d'un groupe produit $G \times G'$ est-il nécessairement le produit de deux sous groupes de G et G' ?

Exercice 4 : Transport de structure
Pour $(x,y) \in \mathbb{R}^2$, on pose $x \star y = x\sqrt{1+y^2} + y\sqrt{1+x^2}$.

1) Vérifier que $\sqrt{1+(x\star y)^2} = \sqrt{1+x^2}\sqrt{1+y^2} + xy$.

2) Montrer que $(\mathbb{R}, \star)$ est un groupe.

3) Montrer que l'application sh est un isomorphisme entre $(\mathbb{R},+)$ et $(\mathbb{R},\star)$.

Exercice 5 : Soit $(G,*)$ un groupe et A une partie non vide de G. On suppose que A est finie et stable par $*$.
Montrer que A est un sous-groupe de G.

Exercice 6 : Soit G un groupe fini et H, K deux sous-groupes de G. On considère l'application $\phi H \times K \to G$ définie par $\phi(h,k) = hk$

1. Est-ce que ϕ est un morphisme de groupes ?
2. Soit $z \in HK$, $z = h_0 k_0$ avec $h_0 \in H$ et $k_0 \in K$.
   Montrer que les antécédents de z par ϕ sont les couples $(h_0 t, t^{-1} k_0)$ avec $t \in H \cap K$.
3. En déduire que : $Card(HK)Card(H \cap K) = Card(H)Card(K)$.
4. Montrer que : (HK est un sous-groupe de G) $\Longleftrightarrow$ $(HK \subset KH)$ $\Longleftrightarrow$ $(HK = KH)$.

Exercice 7 : Sous-groupes d'un groupe cyclique
Soit $n \in \mathbb{N}^*$ et $G = \mathbb{Z}/n\mathbb{Z}$. Soit $k \in \mathbb{Z}$ et $d = k \wedge n$.

1) Déterminer l'ordre de $\overline{k}$ dans G.

2) Montrer que $\overline{k}$ et $\overline{d}$ engendrent le même sous-groupe de G.

3) Quels sont tous les sous-groupes de G ?

Exercice 8 : Groupes d'ordre 6
Déterminer tous les groupes finis de cardinal 6. *(on admettra que dans un tel groupe, il existe un élément a d'ordre 2, et un élément b d'ordre 3).*

Exercice 9 : Soit $(G, .)$ un groupe cyclique de cardinal n.
Montrer, que pour tout diviseur $d \in \mathbb{N}$ de n, G possède un et un seul sous-groupe de cardinal d.

Exercice 10 : Soit G un ensemble fini muni d'une loi de composition interne $*$, associative et telle que tous les éléments sont réguliers.

Montrer que $(G, *)$ est un groupe.

Exercice 11 : Soit $E =]-1, 1[$. On définit la loi $*$ par

$$\forall (x, y) \in E^2 \quad x * y = \frac{x + y}{1 + xy}$$

Montrer que $(E, *)$ est un groupe abélien isomorphe à $(\mathbb{R}, +)$.

Exercice 12 : Soit n un entier supérieur ou égal à 2. Pour tout entier a trouver l'ordre de $\overline{a}$ dans $(\mathbb{Z}/nZ, +)$.

Exercice 13 : Soit $(G, .)$ un groupe. On considère a et b deux éléments de G d'ordres respectifs p et q.

1) On suppose que a et b commutent et que $p \wedge q = 1$. Montrer que ab est d'ordre pq.

2) On suppose encore que a et b commutent.

a) Montrer que si d est un diviseur de p, il existe un élément d'ordre d.

b) Montrer qu'il existe un élément d'ordre $p \vee q$.

3) a) On ne suppose plus $p \wedge q = 1$. Montrer que ab n'est pas nécessairement d'ordre pq, ni d'ordre $p \vee q$.

b) Dans $(\mathscr{G}l_2(\mathbb{R}), \times)$, on considère $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. Montrer que A et B sont d'ordres finis premiers entre eux, mais que AB est d'ordre infini.

Exercice 14 : Soit $(G, .)$ un groupe abélien d'ordre pq, où p et q sont deux nombres premiers distincts.

1) Montrer que G est cyclique.

2) Donner un exemple dans lequel ce résultat peut tomber en défaut si l'on ne suppose pas que G est abélien.

Exercice 15 : Soit $(G, .)$ un groupe d'ordre $2p$, avec p premier.
Montrer que G contient un élément d'ordre p.

3 Anneaux

Exercice 16 : Sommes de nombres impairs

Soit $n \in \mathbb{N}$, $n \geq 2$. Montrer que si N est la somme de n nombres impairs consécutifs, alors N n'est pas premier.

Exercice 17 : Petit théorème de Fermat

Soit $p \in \mathbb{N}$ premier. Montrer que pour $1 \leq k \leq p-1$, p divise $\binom{p}{k}$.

En déduire que $\forall\ n \in \mathbb{Z}$, $n^p \equiv n[p]$.

Exercice 18 : Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. Montrer que : $a \equiv b[n] \Rightarrow a^n \equiv b^n[n^2]$.

Exercice 19 : Soit p et q deux entiers naturels non nuls premiers entre eux.

Montrer que $(X-1)(X^{pq}-1)$ est divisible par $(X^p-1)(X^q-1)$.

Exercice 20 : Caractéristique
Soit A un anneau. On appelle *caractéristique de A* l'ordre de 1 dans le groupe additif $(A, +)$. On suppose A de caractéristique finie, n.

1) Montrer que : $\forall\ x \in A,\ nx = 0$.

2) Si A est intègre, montrer que n est un nombre premier.

3) Si A est intègre et commutatif, montrer que $x \mapsto x^n$ est un morphisme d'anneau.

Exercice 21 : On appelle nilradical d'un anneau commutatif $(A, +, \times)$ l'ensemble N formé des éléments nilpotents de A, c'est à dire des $x \in A$ tels qu'il existe $n \in \mathbb{N}$ vérifiant $x^n = 0$.
Montrer que N est un idéal de A.

Exercice 22 : Soit $(A, +, .)$ un anneau commutatif et I un idéal de A.
On note $\sqrt{I} = \{x \in A \,/\, \exists n \in \mathbb{N}^* \text{ tq } x^n \in I\}$ (radical de I).

1) Montrer que $\sqrt{I}$ est un idéal de A.

2) Montrer que $\sqrt{\sqrt{I}} = \sqrt{I}$.

3) Montrer que $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$ et $\sqrt{I + J} \supset \sqrt{I} + \sqrt{J}$.

4) Exemple : $A = \mathbb{Z}$, $I = 3648\mathbb{Z}$. Trouver $\sqrt{I}$.

Exercice 23 : Un idéal I d'un anneau A est dit premier si :

$$\forall (x, y) \in I^2, \qquad xy \in I \Longrightarrow x \in I \text{ ou } y \in I$$

1) Quels sont les idéaux premiers de $\mathbb{Z}$?

2) Montrer que si A est non nul et si tous les idéaux de A sont premiers alors A est un corps.

Exercice 24 : Soit p un nombre premier différent de 2 et de 5.
Montrer que p divise l'un des éléments de l'ensemble $\{1, 11, 111, 1111, ...\}$.

Exercice 25 : Résoudre dans $\mathbb{Z}^2$ les équations suivantes :

1) $95x + 71y = 46$

2) $20x - 53y = 3$

Exercice 26 : Une bande de 17 pirates dispose d'un butin composé de N pièces d'or d'égale valeur. Ils décident de se le partager également et de donner le reste au cuisinier (non pirate). Celui ci reçoit 3 pièces. Mais une rixe éclate et 6 pirates sont tués. Tout le butin est reconstitué et partagé entre les survivants comme précédemment ; le cuisinier reçoit alors 4 pièces. Dans un naufrage ultérieur, seuls le butin, 6 pirates et le cuisinier sont sauvés. Le butin est à nouveau partagé de la même manière et le cuisinier reçoit 5 pièces. Quelle est alors la fortune minimale que peut espérer le cuisinier lorsqu'il décide d'empoisonner le reste des pirates ?

Exercice 27 : On note $(\mathbb{Z}/3\mathbb{Z})[i] = \left((\mathbb{Z}/3\mathbb{Z})^2, +, *\right)$, où l'addition et la multiplication sont définis de la manière suivante :

$$\forall\,((a,b),(c,d)) \in (\mathbb{Z}/3\mathbb{Z})[i] \quad \begin{cases} (a,b) + (c,d) = (a+c, b+d) \\ (a,b) * (c,d) = (ac - bd, bc + ad) \end{cases}$$

Montrer que ces lois donnent à $(\mathbb{Z}/3\mathbb{Z})[i]$ une structure de corps dont la caractéristique est 3.

Exercice 28 : Soit I un idéal de l'anneau produit $(\mathbb{Z}^2, +, \times)$.

1) On pose $I_1 = \{x \in \mathbb{Z}/(x, 0) \in I\}$ et $I_2 = \{y \in \mathbb{Z}/(0, y) \in I\}$.
Montrer que I_1 et I_2 sont des idéaux de $(Z, +, \times)$.

2) Etablir $I = I_1 \times I_2$.

3) Conclure que les idéaux de l'anneau $(\mathbb{Z}^2, +, \times)$ sont de la forme $x\mathbb{Z}^2$ avec $x \in \mathbb{Z}^2$.

4 Polynômes

Exercice 29 : Endomorphisme $P \mapsto AP[B]$
Soit $E = \mathbb{K}_3[X]$, $A = X^4 - 1$, $B = X^4 - X$, et φ l'application de E dans E qui à P associe le reste de la division euclidienne de AP par B.
Chercher $\ker(\varphi)$, $\mathrm{Im}(\varphi)$.

Exercice 30 : Calcul de pgcd
Calculer le pgcd de P et Q pour :

a) $P = X^4 + X^3 - 3X^2 - 4X - 1$
$Q = X^3 + X^2 - X - 1$

b) $P = X^4 - 10X^2 + 1$
$Q = X^4 - 4X^3 + 6X^2 - 4X + 1$

c) $P = X^5 - iX^4 + X^3 - X^2 + iX - 1$
$Q = X^4 - iX^3 + 3X^2 - 2iX + 2$

Exercice 31 : Coefficients de Bézout

Montrer que les polynômes P et Q suivants sont premiers entre eux. Trouver $U, V \in \mathbb{K}[X]$ tels que $UP + VQ = 1$.

a) $P = X^4 + X^3 - 2X + 1$
$Q = X^2 + X + 1$

b) $P = X^3 + X^2 + 1$
$Q = X^3 + X + 1$

Exercice 32 : Soit $P \in \mathbb{K}[X]$. Démontrer que $(P(X) \wedge P(-X))$ et $(P(X) \vee P(-X))$ sont pairs ou impairs.

Exercice 33 : Lemme de Gauss

Soit $P \in \mathbb{Z}[X]$. On appelle *contenu de* P le pgcd des coefficients de P (notation : $\text{cont}(P)$).

1) Soient $P, Q \in \mathbb{Z}[X]$ avec $\text{cont}(P) = 1$, et $R = PQ$. Soit p un facteur premier de $\text{cont}(R)$.

a) Si p est premier avec le coefficient constant de P, Démontrer que p divise tous les coefficients de Q.

b) Si p divise le coefficient constant de P, se ramener au cas précédent.

c) En déduire que $\text{cont}(Q) = \text{cont}(R)$.

2) Lorsque $\text{cont}(P) \neq 1$, trouver $\text{cont}(PQ)$.

3) Application : Soit $R \in \mathbb{Z}[X]$, et $P, Q \in \mathbb{Q}[X]$ tels que $R = PQ$. Montrer qu'il existe $P_1, Q_1 \in \mathbb{Z}[X]$ proportionnels à P et Q et tels que $R = P_1 Q_1$.
(*c'est-à-dire : un polynôme à coefficients entiers réductible sur* $\mathbb{Q}$ *est aussi réductible sur* $\mathbb{Z}$)

5 Avec Python

Exercice 34 : Dans tout ce sujet n désigne un naturel non nul.

On note $\varphi(n)$ l'indicatrice d'Euler de n, U_n l'ensemble des racines n-ième de l'unité et U_n^* l'ensemble des racines de l'unité d'ordre exactement n. Enfin, pour $d \in \mathbb{N}^*$, on pose

$$\Phi_d = \prod_{z \in U_d^*} (X - z)$$

1) Écrire en Python la fonction `liste(n)` qui renvoie

$$\{k \in [\![1, n]\!] \ / \ k \wedge n = 1\}$$

Écrire la fonction `phi(n)` qui renvoie $\varphi(n)$ puis `sumphi(n)` qui renvoie

$$\sum_{d|n} \varphi(d)$$

2) Montrer

$$X^n - 1 = \prod_{d|n} \Phi_d$$

3) Justifier

$$\sum_{d|n} \varphi(d) = n$$

4) Montrer que Φ_n est un polynôme à coefficients entiers.

On pose $Q_n = X^n - 1$ et on choisit p, q, r des nombres premiers vérifiant

$$p < q < r < p + q$$

On pose

$$n = pqr \text{ et } R = \frac{Q_p Q_q Q_r}{X - 1}$$

5) Montrer

$$\Phi_n = \frac{Q_n R}{Q_{pq} Q_{qr} Q_{rp}}$$

6) Montrer qu'il existe un polynôme S tel que

$$\Phi_n - R = X^{pq} S$$

7) En déduire que le coefficient de X^r dans Φ_n est égal à -2.

Exercice 35 : Fonction et inversion de Möbius

On appelle fonction de Möbius l'application $\mu : \mathbb{N}^* \to \{-1, 0, 1\}$ définie par

$$\mu(1) = 1, \quad \forall n \in \mathbb{N} \setminus \{0,1\} \begin{cases} \mu(n) = (-1)^r \text{ si } n \text{ est le produit de } r \text{ nombres premiers 2 à 2 distincts} \\ \mu(n) = 0 \text{ si } n \text{ est divisible par le carré d'un nombre premier} \end{cases}$$

1) Montrer que μ est une fonction multiplicative, c'est-à-dire : $\mu(1) = 1$ et, si a et b sont premiers entre eux, $\mu(ab) = \mu(a)\mu(b)$.

2) On note $d|n$ pour signifier que l'entier naturel d non nul divise $n \in \mathbb{N}^*$. Montrer que

$$\forall n \geqslant 2 \qquad \sum_{d|n} \mu(d) = 0$$

3) Ecrire une fonction `Python`, `mu`, de variable n, qui calcule $\mu(n)$.
La tester pour $n \in [\![1, 20]\!]$.

4) Soit f une application de $\mathbb{N}^*$ dans $\mathbb{R}$. On définit pour tout $n \in \mathbb{N}^*$: $g(n) = \sum_{d|n} f(d)$.

(a) Ecrire une fonction `Python` de paramètres f et n qui calcule $g(n)$.

(b) Exemple : on considère f définie par $f : n \mapsto n^3 - 2n - 1$.
Calculer, pour $n \in [\![1, 20]\!]$, $\sum_{d|n} \mu(d) g\left(\frac{n}{d}\right)$ et $f(n)$.

(c) Montrer le résultat qui apparait.

6 Polynômes

Exercice 36 : Endomorphisme $P \mapsto AP\ [B]$

Soit $E = \mathbb{K}_3[X]$, $A = X^4 - 1$, $B = X^4 - X$, et φ l'application de E dans E qui à P associe le reste de la division euclidienne de AP par B.
Chercher $\ker(\varphi)$, $\mathrm{Im}(\varphi)$.

Exercice 37 : Calcul de pgcd

Calculer le pgcd de P et Q pour :

a) $P = X^4 + X^3 - 3X^2 - 4X - 1$
$Q = X^3 + X^2 - X - 1$

b) $P = X^4 - 10X^2 + 1$
$Q = X^4 - 4X^3 + 6X^2 - 4X + 1$

c) $P = X^5 - iX^4 + X^3 - X^2 + iX - 1$
$Q = X^4 - iX^3 + 3X^2 - 2iX + 2$

Exercice 38 : Montrer que les polynômes P et Q suivants sont premiers entre eux. Trouver $U, V \in \mathbb{K}[X]$ tels que $UP + VQ = 1$.

a) $P = X^4 + X^3 - 2X + 1$
$Q = X^2 + X + 1$

b) $P = X^3 + X^2 + 1$
$Q = X^3 + X + 1$

Exercice 39 : Soit $P \in \mathbb{K}[X]$. Démontrer que $(P(X) \wedge P(-X))$ et $(P(X) \vee P(-X))$ sont pairs ou impairs.

Exercice 40 : Soient $n \in \mathbb{N}$, et $t_0, t_1, ..., t_n$ $n+1$ réels 2 à 2 distincts. On note L_0, L_1, ..., L_n les polynômes de Lagrange associés.

1) Pour $p \leq n$, exprimer le polynôme X^p en fonction de L_0, L_1, ..., L_n.

En déduire la valeur de $\sum_{j=0}^{n} t_j^p L_j(0)$.

2) Trouver un polynôme P de degré n tel que $\forall j \in \{0,1,...,n\}, P(t_j) = t_j^{n+1}$.

En déduire la valeur de $\sum_{j=0}^{n} t_j^{n+1} L_j(0)$.

7 Avec Python

Exercice 41 : Dans tout ce sujet n désigne un naturel non nul.

On note $\varphi(n)$ l'indicatrice d'Euler de n, U_n l'ensemble des racines n-ième de l'unité et U_n^* l'ensemble des racines de l'unité d'ordre exactement n. Enfin, pour $d \in \mathbb{N}^*$, on pose

$$\Phi_d = \prod_{z \in U_d^*} (X - z)$$

1) Écrire en Python la fonction `liste(n)` qui renvoie

$$\{k \in [\![1,n]\!] \ / \ k \wedge n = 1\}$$

Écrire la fonction `phi(n)` qui renvoie $\varphi(n)$ puis `sumphi(n)` qui renvoie

$$\sum_{d|n} \varphi(d)$$

2) Montrer

$$X^n - 1 = \prod_{d|n} \Phi_d$$

3) Justifier

$$\sum_{d|n} \varphi(d) = n$$

4) Montrer que Φ_n est un polynôme à coefficients entiers.

On pose $Q_n = X^n - 1$ et on choisit p, q, r des nombres premiers vérifiant

$$p < q < r < p + q$$

On pose

$$n = pqr \text{ et } R = \frac{Q_p Q_q Q_r}{X - 1}$$

5) Montrer

$$\Phi_n = \frac{Q_n R}{Q_{pq} Q_{qr} Q_{rp}}$$

6) Montrer qu'il existe un polynôme S tel que

$$\Phi_n - R = X^{pq} S$$

7) En déduire que le coefficient de X^r dans Φ_n est égal à -2.

Exercice 42 : Fonction et inversion de Möbius

On appelle fonction de Möbius l'application $\mu : \mathbb{N}^* \to \{-1, 0, 1\}$ définie par

$$\mu(1) = 1, \quad \forall n \in \mathbb{N} \setminus \{0,1\} \begin{cases} \mu(n) = (-1)^r \text{ si } n \text{ est le produit de } r \text{ nombres premiers 2 à 2 distincts} \\ \mu(n) = 0 \text{ si } n \text{ est divisible par le carré d'un nombre premier} \end{cases}$$

1) Montrer que μ est une fonction multiplicative, c'est-à-dire : $\mu(1) = 1$ et, si a et b sont premiers entre eux, $\mu(ab) = \mu(a)\mu(b)$.

2) On note $d|n$ pour signifier que l'entier naturel d non nul divise $n \in \mathbb{N}^*$. Montrer que

$$\forall n \geqslant 2 \qquad \sum_{d|n} \mu(d) = 0$$

3) Ecrire une fonction `Python`, `mu`, de variable n, qui calcule $\mu(n)$.
La tester pour $n \in [\![1, 20]\!]$.

4) Soit f une application de $\mathbb{N}^*$ dans $\mathbb{R}$. On définit pour tout $n \in \mathbb{N}^*$: $g(n) = \sum_{d|n} f(d)$.

(a) Ecrire une fonction `Python` de paramètres f et n qui calcule $g(n)$.

(b) Exemple : on considère f définie par $f : n \mapsto n^3 - 2n - 1$.
Calculer, pour $n \in [\![1, 20]\!]$, $\sum_{d|n} \mu(d) g\left(\frac{n}{d}\right)$ et $f(n)$.

(c) Montrer le résultat qui apparait.